GlobalResearch
Center for Research on Globalization

Beyond Star Wars, America Seeks Hegemony in Cyberwarfare

By Prof. Igor Panarin
Global Research, January 11, 2012
Russia Today and Stop NATO 11 January 2012

Theme: Militarization and WMD, US NATO War Agenda

The NSA performs clandestine surveillance of Russia's electronic communications through Echelon elements stationed in Norway, Cyprus, Kyrgyzstan and the Baltic states.

The US Cyber Command, aka CYBERCOM, plans to employ cyber warfare for purposes of land-based, naval and aerial military operations.

[O]n 5 January 2012 President Obama and the DoD released a defense strategic guidance titled "Sustaining US Global Leadership: Priorities for 21st-century Defense." The document formulates the United States' top strategic priority as securing the nation's global dominance through aggressive action in cyberspace. Herein, the White House and the Pentagon explicitly state their intention to enhance America's global posture by securing its domination in cyberspace through information and cyber warfare tactics.

Thus, the Obama administration is laying out its own ambitious global-domination project, superseding Ronald Reagan's "Star Wars" and George Bush Junior's "War on Terror": a global war in cyberspace.

US President Obama delivered a public address in the Pentagon on 5 January this year introducing the "defense strategic review." Writer and political analyst Igor Panarin believes Washington's new military doctrine will focus on cyberspace supremacy.

The United States was first to approach cyberspace as a new sphere of military action, along with the existing military domains such as land, sea, air and space. The concept dates back to 1998, but it was only developed into a concrete action plan following the war in South Ossetia in August 2008, which did not play out well for the US and its Georgian proxy.

Late in May 2009, President Barack Obama instituted the post of Cyberspace Coordinator within his administration, with the coordinator sitting on both the National Security Council and the National Economic Council. The same month saw the establishment of the US Cyber Command, headquartered at Fort Meade, Maryland, and headed by Army General Keith Alexander, who also happens to be the head of the National Security Agency, America's most powerful intelligence service.

The National Security Agency/Central Security Service (NSA/CSS) is the United States' centermost intelligence agency. It was formally established on 4 November 1952. The agency is responsible for the collection of foreign communications and signals intelligence, employing the Echelon eavesdropping system as its key technical asset. The NSA performs

clandestine surveillance of Russia's electronic communications through Echelon elements stationed in Norway, Cyprus, Kyrgyzstan and the Baltic states.

The US Cyber Command, aka CYBERCOM, plans to employ cyber warfare for purposes of land-based, naval and aerial military operations. Special information and cyber warfare units and command structures have been set up within the US armed forces, including the Army Cyber Command/Second Army. Naval cyber warfare is to be directed through the Fleet Cyber Command, based on the once-disbanded and specially reestablished US 10th Fleet. The air force component of CYBERCOM is the 24th Air Force, aka Air Forces Cyber. The US Marine Corps also has its own Cyberspace Command.

The US Department of Defense's technical research branch, the Defense Advanced Research Projects Agency (DARPA) is currently finalizing its National Cyber Range: a miniature version of the internet meant as a testing ground for cyber intelligence and warfare. The Cyber Range is intended for testing new tactics and techniques through cyber war games, as well as for training cyber troops. The new strategy also includes developing new cyber weapons and tools, such as passive viruses, cyber beacons, etc.

US lawmakers have already developed new legislation regulating government and military activities aimed at securing America's cyberspace supremacy.

One of the notable trends is simplified decision making for offensive cyber warfare operations and activities. In the past, launching a cyber attack required stage-by-stage authorization from the Joint Chiefs of Staff, then the defense secretary, and then the US president. Under the new rules, decision making on such an action will take no more than 10 minutes. This primarily concerns psychological operations targeting any specific audience of Internet users.

CYBERCOM held a simulation exercise early in December 2011, which eventually earned praise from Gen. Alexander. The exercise involved 300 cyber specialists designated respectively as CYBERCOM elements and "the enemy," practicing offensive and defensive tactics and coordination. The simulated US cyber defense operation was centered at the Air Force's Nevada Test and Training Range at Nellis, Nevada, while the designated aggressors sought to penetrate the American cyber network from remote locations.

In just over a week, both sides sought to win the initiative and counter each other's moves, analyzing their own progress and performance through daily operational briefings. The exercise served to try out various real-time scenarios based on the probable action and counter-action of a potential adversary. DoD officials commended the exercise as highly successful, complimenting CYBERCOM specialists for their proficiency and excellent teamwork.

Rather mysteriously, the CYBERCOM exercise took place at the same time as Russia experienced an unprecedented surge in street protests following its parliamentary election last December. It seems rather telling that the protest rallies that drew thousands of people in some of Russia's major cities were mainly organized and dispatched through web-based social networks such as Facebook.

Finally, on 5 January 2012 President Obama and the DoD released a defense strategic guidance titled "Sustaining US Global Leadership: Priorities for 21st-century Defense." The document formulates the United States' top strategic priority as securing the nation's global

dominance through aggressive action in cyberspace. Herein, the White House and the Pentagon explicitly state their intention to enhance America's global posture by securing its domination in cyberspace through information and cyber warfare tactics.

Thus, the Obama administration is laying out its own ambitious global-domination project, superseding Ronald Reagan's "Star Wars" and George Bush Junior's "War on Terror": a global war in cyberspace.

Stop NATO e-mail list home page with archives and search engine:
http://groups.yahoo.com/group/stopnato/messages

Stop NATO website and articles:
http://rickrozoff.wordpress.com

To subscribe for individual e-mails or the daily digest, unsubscribe, and otherwise change subscription status:
stopnato-subscribe@yahoogroups.com

Articles by: Prof. Igor Panarin